REMARKS

Initially, in the Office Action dated December 31, 2003, the Examiner objects to claims 3, 5, 6, 8, 16, 17, 20, 21, 27, 30 and 31 because of informalities. The specification has been objected to because of the use of the trademark BLUETOOTH without capitalizing it.

Claim 27 has been rejected under 35 U.S.C. §112, second paragraph. Claims 1-11, 13, 18 and 28-31 have been rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,163,147 (Orita). Claim 12 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of WO 99/00958 (Leveridge et al.). Claims 14-17 and 20-26 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of BLUETOOTH: Visions, Goals and Architecture (Haartsen et al.). Claims 19 and 27 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of U.S. Patent No. 5,818,936 (Mashayekhi).

By the present response, Applicants have amended the specification to further clarify the invention. Further, Applicants have amended claims 3, 5, 6, 8, 16, 17, 20, 21, 27, 30 and 31 to further clarify the invention. Applicants have submitted new claim 32 for consideration by the Examiner and assert that this claim does not contain any prohibited new matter. Claims 1-32 remain pending in the present application.

Information Disclosure Statement

Applicants apologize for any inconvenience caused the Examiner by the inadvertent omission of a copy of reference AW. Applicants appreciate the Examiner's retrieval of a copy of this reference, and its consideration.

Claim Objections

Claims 3, 5, 6, 8, 30 and 31 have been objected to because of informalities. Applicants have amended these claims to further clarify the invention and respectfully request that these objections be withdrawn.

Specification Objections

The Examiner has requested that the term "BLUETOOTH" be capitalized asserting that this is a trademark. Applicants have amended the specification to comply with the Examiner's request and respectfully request that these objections be withdrawn.

35 U.S.C. §112 Rejections

Claim 27 has been rejected under 35 U.S.C. §112, second paragraph. Applicants have amended this claim to further clarify the invention and respectfully request that this rejection be withdrawn.

35 U.S.C. §102 Rejections

Claims 1-11, 13, 18 and 28-31 have been rejected under 35 U.S.C. §102(b) as being anticipated by Orita. Applicants respectfully traverse these rejections.

Orita discloses a computer system with file security function where environment profile information defining a file to be accessed and an executable user

program are previously stored in a storage unit. The environment profile information is selected by operator profile information corresponding to ID information input via a workstation by a user. A host computer executes the user program defined by the environment profile information. When a specified file access is requested after the execution of the user program, whether execution of the file access is permitted or not is determined according to access protection information. The access protection information is information having access types and file contents defined by the environment profile information.

Regarding claims 1, 27, 28, 30, 31 and new claim 32, Applicants submit that Orita does not disclose or suggest the limitations in the combination of each of these claims of, inter alia, access control means accessible by a communicating device requesting access to a first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, arbitrating the access of a requesting device to a service provided to a providing device that includes determining, in an arbitration means, whether to grant or refuse access to a first application by the requesting device, wherein if the determination requires authentication of the requesting device, the authentication is performed during that determination and not previously, arbitration means for determining whether a requesting device communicating through the

interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device wherein if the requesting device has a stored trust indication associated therewith, no user authorization is required, and if the requesting device has no stored trust indication associated therewith, user authorization is requirable. Orita does not disclose or suggest these limitations in the claims of the present application. Orita discloses authentication of the operator always being required (using the ID password) in order to access the host computer 11. According to the disclosure of Orita, it is always necessary for the user to input an ID password in order to gain access to the host computer and storage unit and for the OP and EP information to be downloaded into the RAM area 14 of the host computer 11. Orita does not disclose or suggest access to the host computer without authentication. According to embodiments of the present invention, application-specific access is provided (see Fig. 6, page 12, line 5 - page 14, line 14). This is achieved by allowing access to the access control means without authentication, arbitration at the access control means to determine whether access to a requested application is refused or granted, and performing authentication if the arbitration requires it, as recited in the claims of the present application. In contrast, Orita discloses access to a file being determined by an operator's authority level stored in an EP information file. As noted previously, in Orita, authentication is always required (using the ID password) in order to access the host computer.

The Examiner asserts that Orita discloses access control means accessible by a communicating device requesting access to a first application without the communicating device having been authenticated by the authenticating means, . . . as recited in the claims of the present application, in Orita at col. 1, lines 51-56 and col. 2, lines 10-19. However, these portions of Orita merely disclose a computer system having a security function capable of attaining the security according to the content of a file and the access type at the time of accessing file by a user so as to affect a reliable security operation for files, and that it is determined whether execution of file access is permitted or not based on the access protection information read out from a second storage unit when an access request is made with respect to a specified file stored in a first storage unit according to a user program. This is not a communicating device requesting access to a first application without the communicating device having been authenticated by an authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructing the authentication means to authenticate the communicating device, as recited in the claims of the present application. These portions of Orita do not disclose or suggest a communicating device requesting access to an application, or determining whether a communicating device has been authenticated by an authentication means. Further, these portions of Orita do not disclose or suggest an authentication means to authenticate a communicating device if arbitration requires an authentication of

the communicating device. These portions of Orita merely disclose attaining security according to the content of a file where execution of file access is determined based on the access protection information read out from a storage unit. The claims of the present application relate to access to an application. In contrast, Orita relates to access to a file.

Regarding claims 2-11, 13, 18 and 29, Applicants submits that these claims are dependent on one of independent claims 1 and 28 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. For example, Orita does not disclose or suggest the access control means being arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration.

Accordingly, Applicants submit that Orita does not disclose or suggest the limitations in the combination of each of claims 1-11, 13, 18 and 28-32 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. §103 Rejections

Claim 12 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Leveridge et al. Applicants respectfully traverse this rejection.

Leveridge et al. discloses an authentication server being provided which stores authentication details of authorized users, and a list of currently authenticated

users. A number of application servers are connected to the authentication server, to allow the authentication servers to check the current authentication status of a user which requires service by the application servers. A session key is generated during the authentication procedure, for use during subsequent communications.

Applicants submit that claim 12 is dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Leveridge et al. does not overcome the substantial defects noted previously regarding Orita. For example, none of the cited references disclose or suggest authentication comprising secret key exchange between the device and the communicating device.

Accordingly, Applicants submit that neither Orita nor Leveridge et al. taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 12 of the present application. Applicants respectfully request that this rejection be withdrawn and that this claim be allowed.

Claims 14-17 and 20-26 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Haartsen et al. Applicants respectfully traverse these rejections.

Haartsen et al. discloses the vision and goals of the BLUETOOTH program and introduces the radio-based technology that consists of a low cost, low power radio-based cable replacement. This technology provides a basis for portable devices to communicate together in an ad hoc fashion by creating personal area networks which have similar advantages to their office environment counterpart, the

local area network (LAN). The vision, goals, and architecture of BLUETOOTH are disclosed.

Applicants submit that claims 14-17 and 20-26 are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted regarding this independent claim. Applicants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. For example, Applicants submit that none of the cited references disclose or suggest each multiplexing protocol layer, in the route of the request as it proceeds up through the protocol stack, querying a security manager, which if the requested application is not connected to the querying protocol layer, allows access of the request through the querying protocol layer to a higher multiplexing protocol layer, and, if the requested application is connected to the querying protocol layer, performs an arbitration to grant or refuse access of the communicating device to the requested application.

Accordingly, Applicants submit that neither Orita nor Haartsen et al. taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 14-17 and 20-26 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 19 and 27 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Mashayekhi. Applicants respectfully traverse these rejections.

Mashayekhi discloses a distributed authentication service that automates an authentication exchange between a user and an application program of a distributed network system. The distributed authentication service includes an exchange controller coupled to an authentication database containing a group of encrypted application secrets associated with the user. Each application secret is, in turn, associated with a particular program resident in the system.

Regarding claim 27, Applicants submit that neither Orita nor Mashayekhi, taken alone or in any proper combination, disclose or suggest the limitations in the combination of this claim of, inter alia, first access control means accessible by a communicating device requesting access to the first application program without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, or second access control means accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, wherein the first access control means is accessible by a communicating device requesting access to

the second application without the communicating device having been authenticated by the authentication means, and is arranged to provide the access of the communicating device to the second access control means. As has been noted previously, Orita does not disclose or suggest these limitations in the claims of the present application. The Examiner admits that Orita fails to disclose or suggest a second access control means accessible by a communicating device requesting access to a second application . . . as recited in claim 27 of the present application, but asserts that Mashayekhi teaches these limitations at col. 5, lines 56-60 and col. 6, lines 43-59. However, these portions of Mashayekhi merely disclose that a workstation and server nodes may be configured as a distributed authentication service that automates an authentication exchange between a user interface, and that keychain objects associated with one or more application objects have attributes of at least one application secret and a public/private key pair where the application secret contains data used by a particular program to authenticate a user. Application secrets may be grouped according to access control level for each application program (e.g., requiring administrative rights for modification, allowing user modifications). This is not a second access control means accessible by a communicating device requesting access to a second application without the communicating device having been authenticated and the other associated limitations, as recited in the claims of the present application. These portions of Mashayekhi do not disclose or suggest anything related to arbitrating whether access of a communicating device is granted or refused or if arbitration requires

authentication of a communicating device. Further, these portions of Mashayekhi do not disclose or suggest anything related to a first access control means being accessible by a communicating device requesting access to a second application without the communicating device having been authenticated by an authentication means, and arranged to provide the access of the communicating device to the second access means, as recited in the claims of the present application. As noted, Mashayekhi discloses keychain objects associated with one or more application objects have attributes of at least one application secret and a public/private key pair where the application secret contains data used by a particular program to authenticate a user. The claims of the present application relate to authentication of a communicating device. In addition, Applicants do not interpret these portions of Mashayekhi the way the Examiner interprets it to indicate that once a user has been authenticated to system, the user can be authenticated to all of the other applications.

Regarding claim 19, Applicants submit that dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted regarding this independent claim. For example, Applicants submit that none of the cited references disclose or suggest the plurality of access control means being arranged in an hierarchy wherein a first access control means at the lowest level in the hierarchy provides access to at least a second access control means and access to one or both of a third access control means and an application, wherein access to each application is provided via one or more access control means including the first

application control means and the application's connected access control means, if different, and wherein any access control means is accessible by a communicating device requesting access to one of its connected applications without the communicating device having been authenticated by the authentication means, and being arranged to arbitrate whether access of the communicating device to the one connected application is granted or refused, the connected access control means instructing the authentication means to authenticate the communicating device if the arbitration requires an authentication of the communicating device.

Accordingly, Applicants submit that neither Orita nor Mashayekhi taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 19 and 27 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-32 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 1156.41275X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600